ƒ 4.-

HACK-TIC 4

TIJDSCHRIFT VOOR TECHNO-ANARCHISTEN

Met in dit nummer:

- **Telefooncellen gesaboteerd**
- **Computernetten overzicht**
- **Doorschakelen van telefoonverbindingen**
- **Cursus VMS hacking**
- **Draadloze telefoons**



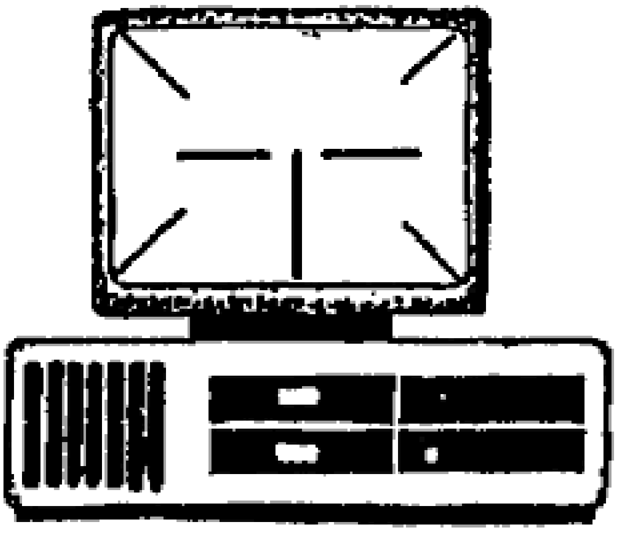
Nederlands Grootste, Dikste, Voordeligste en Kleurrijkste Hacker-blad

COLOFON

HACK-TIC: is Nederlands eerste hackerblad. Naar we hopen verschijnt het ongeveer 10 x per jaar.
UITGAVE: met moeite (door een volkomen ongebonden en ongeorganiseerd gezelschap van vreemde types).
REDAKTIE: Jolanda, The Key, John D., Tx, Herman Acker, Peter Poelman, Paul en Rop.
ILLUSTRATIES: Koen Hottentot.
KONTAKT: De redaktie is te bereiken via p.b. 22953, 1100 DL Amsterdam. UUCP: ..!mcvax!neabbs!rop. Op het FIDO net 2:280/1 Hack Tic. Telex (modern 50 baud telecommunicatiecomfort van de PTT) 12969 neabs nl, telefax 020-763706. Zowel bij telex als bij fax even vermelden dat het voor Hack-Tic is. Ons telefoonnummer is 020-6001480 (abonnee's die zonder dringende reden voor 13:00 uur bellen krijgen hun volgende nummers met strafport).
PRIJS: Losse nummers kosten 4 gulden, een abonnement voor 10 nummers (moet ongeveer een jaar meegaan) kost ƒ 37.50, Abonnementsgelden overmaken op bankrekeningnummer 98.72.84.541 t.n.v. Rop Gonggrijp. Rekening loopt bij de verenigde spaarbank, postrek. no. 15368. Abonnementen beginnen met het laatst uitgegeven nummer tenzij je bij de betaling een ander beginnummer aangeeft. Oude nummers die niet meer voorradig zijn worden ook niet in rekening gebracht.
PRIVACY: Het is waar: als "ze" willen, hoeven ze alleen maar naar onze bankafschriften te kijken om te zien wie er abonnee zijn. Wij vinden Hack-Tic een uiterst onschuldig blaadje, maar de kans bestaat dat lokale, regionale, nationale en in de toekomst wellicht zelfs Europese overheden het daar niet mee eens zijn. Heb je een maatschappelijke positie die je niet wilt verliezen dan kun je ook geld of girocheque en adres bijsluiten in een envelop en die aan onze postbus sturen, wij weten dan genoeg. De Hack-Tic wordt altijd verstuurd in een neutrale envelop. (Straks denkt je hospita nog dat je porno koopt per postorder). Hack-Tic is ook verkrijgbaar bij de goede boekhandel (wellicht herkenbaar aan het observatieteam voor de deur).
DISCLAIMER: Informatie in Hack-Tic dient slechts een educatief doel. Gebruik van deze informatie zou strafbaar/staatsgevaarlijk/stout kunnen zijn. De redaktie wijst iedere verantwoordelijkheid voor gebruik door lezers van de in Hack-Tic opgenomen informatie af.
NADRUK: toegestaan! Kranten, tijdschriften, omroepstichtingen, politieke partijen, wasmachinereparateurs etc. etc. mogen zonder voorafgaande toestemming van de redaktie (maar natuurlijk met bronvermelding) stukken overnemen uit de Hack-Tic. De bovenstaande disclaimer blijft echter van kracht. Nadruk van de gehele Hack-Tic is na-

tuurlijk verboden. (Neem toch maar een abonnement, want wij hebben hier een kooi vol goeie advokaten die al weken niets meer gegeten hebben.)
NABESTELLEN: Oude nummers kosten ook fl. 4,- (voor zover voorradig) en kunnen via de postbus besteld worden.
HOE: Hack-Tic werd met het WYSMRWYG (What You See Might Resemble What You Get) DTP pakket Ventura 2.0 gemaakt op een gammele AT. Print-outs van elke pagina gemaakt met zo'n modern lasergeval gezoeft en daarna met een Multilith-1250 offsetpers vermenigvuldigd (met dank aan Pieter, onze drukker). Dan nog even laten vouwen, nieten en snijden en klaar was Kees (hopen we terwijl we dit tikken).
VERKRIJGBAAR: moeilijk, maar wellicht bij: Het Computercollectief, Cafka computers, Fort van Sjakoo, Slagerzicht en Athenaeum Boekhandel, allen in Amsterdam, De Rode Hond en Meek-It in Den Haag, De Rooie Rat in Utrecht, De Denker in Nijmegen en Athenaeum in Haarlem.

IN DEZE TIC:



Hack-Tic administratie

Deze hack-Tic verschijnt iets later dan gepland maar hij is - om je te troosten - dit keer geheel gedrukt in plaats van gekopieerd. Verder hebben we de gebruikelijke administratieachterstand.

Het begint dan wel te lijken op een echte administratie, maar we zijn er nog lang niet. We vragen nog steeds een beetje begrip voor wantoestanden alhier. Niet schieten, we doen ons best.

Mensen die niets of te weinig hebben ontvangen kunnen bellen met 020-6001480 om de zaak recht te zetten. Mensen die te veel hebben ontvangen kunnen een wiend/in een plezier doen.

Er komen ook nogal wat klachten binnen van mensen die denken dat de Hack-Tic elke maand verschijnt en die daarom graag het nummer van april willen hebben. Nogmaals: we verschijnen ONGEVEER elke vijf weken. Externe factoren zoals strandweer, eindexamens en humeur hebben echter onvermijdelijk enige invloed op het verschijningsritme van de Tic. Een echte hacker kent zichzelf goed genoeg om dit ongemak voor lief te nemen, zo vinden wij.

Nog wat: We krijgen nogal wat chequebetalingen binnen waarop geen adres is vermeld. Wij kunnen dan wel veel moeite gaan doen om het adres te achterhalen, op het moment zijn we door tijdgebrek gedwongen te wachten tot de abonnee iets van zich laat horen (tot die tijd innen we de cheque natuurlijk niet). Als je nog niets hebt ontvangen (en je ziet deze Hack-Tic ergens liggen), bel dan snel.

Tot slot nog even voor onze Belgische abonnee's (we hebben ze!): betaal in godsnaam niet met een bankcheque, eurocheque of iets in die richting, want dat kost hier minstens fl. 30,- om te innen, en dat wordt ons toch iets te gek. Het beste kun je proberen het geld direkt op onze bankrekening te laten belanden. Je kunt ook Bfr.750 bijsluiten in een envelop en die opsturen naar onze postbus.

Namens redaktie & administratie,

Jolanda

Lezerspost

Beste mede-Techno-Anarchisten,

Na het lezen van de Hack-tic stonden er grote ??? in mijn ogen. Het is allemaal best leuk wat jullie schrijven, maar voor een toekomstig Hacker staat er absoluut niets in. Daarom een paar vraagjes:

- **Welk modem is goedkoop, geschikt en snel - 2400 baud is een bekende kreet - genoeg? (waar krijg ik het etc.?)**
- **Hoe kom ik in een mailbox, wat kost dat (wat zijn de truukjes om er gratis in te komen - I'm just a poor student suffering from Dect-mano-phagie!)**
- **Wat is nu eigenlijk FIDO of ISDN?**
- **Hoe kan ik - being a DOSser - met VAX, PDP etc. communiceren. Het HACKZO artikel laat genoeg voorbeelden zien van dingen die ik absoluut niet begrijp.**

Let this loner get social!!

Christian van Hoven, Nijmegen

We denken dat het niet onze taak is om modems of andere randapparatuur te bespreken: diverse andere bladen doen hun best elke maand het volledige hardware-assortiment te testen of anderzins te bespreken.

Er zijn voor de beginner bladen genoeg; Hack-Tic probeert ook voor de wat verder gevorderde computergebruiker interessant te zijn, wat tot gevolg heeft dat er zo nu en dan voor veel mensen onbegrijpelijke artikelen in staan. We proberen natuurlijk wel om de informatie zo helder mogelijk te brengen.

In Hack-Tic 1 staat een groot artikel over NEABBS, Nederlands grootste Bulletin Board Systeem (mailbox dus). NEABBS kost geld. Er zijn in Nederland zo'n 250 systemen dag en nacht bereikbaar, dus er is keus genoeg. Er zijn ook veel systemen die geen geld vragen, maar die zitten vaak niet op allerlei netwerken aangesloten, en daar is dus minder informatie voorhanden.

FIDO is een netwerk van bulletin boards die onderling berichten met elkaar uitwisselen. In Nederland wordt dit netwerk gerund door de Hobby Computer Club, de officiële, erkende, niet-kopieërende, keurige en brave PC-hobbyisten. Dit komt de kwaliteit van de berichten op het FIDO-net op zijn zachtst gezegd niet ten goede.

ISDN staat voor Integrated Services Digital Network, een plan om alle telecommunicatie in 1 net te stoppen en dat alles door een glasvezel naar de abonnee toe te brengen. Dit komt nog een keer uitgebreid aan de orde.

Over Vax/VMS hebben we deze week een artikel dat je vertrouwd zou moeten maken met de basisprincipes van het VMS operating system. Zowel de VAX als de PDP zijn machines (beide van Digital), het gaat er om welk OS ze draaien.

AMRO betaaldiskette

De AMRO bank levert een programma waarmee bedrijven zelf hun betalingen op diskette kunnen zetten. Dit programma is met een wachtwoord beveiligd. De beveiliging werkt (aldus de anonieme inzender van deze informatie) als volgt:

Het programma maakt een "CONFIG.MEM" file aan waarin diverse variabelen betreffende de gebruiker zijn weggeschreven (men gebruikt de taal Clipper, de DBase compiler), en wel 22 tekens achter de veldnaam. De namen voor die wachtwoorden zijn resp. CONFIG_COP & CONFIG_PAS. De code is weggeschreven als nummerieke string met een maximum lengte van 50 tekens.

De code is als volgt opgebouwd: het password bestaat uit 6 letters. Deze zijn omgezet in hun binaire ASCII waarde. Bijv. A = 01000001. De code voor deze letter is dan 260, waarbij het eerste cijfer (2) het aantal enen aangeeft en de volgende 2 cijfers de positie van die enen in de tekenrij (bit 6 en bit 0). Een eenvoudige omzetting maakt dit leesbaar. Een ander voorbeeld: 2632603610463103620364l wordt dus

263	=01001000	= CHR$(72)	= "H"
260	=01000001	= CHR$(65)	= "A"
3610	=01000011	= CHR$(67)	= "C"
46310	=01001011	= CHR$(75)	= "K"
3620	=01000101	= CHR$(69)	= "E"
3641	=01010010	= CHR$(82)	= "R"

Anoniem ingezonden.



Wat we nou toch in onze electronische postbus vonden! Enkele ijverige Hack-Tic abonnee's blijken een truukje te hebben gevonden om door middel van het doorknippen van een draadje gratis te kunnen bellen vanuit een telefooncel. Hoewel dit alles ontzettend strafbaar is geeft het goed aan wat de PTT bedoelt met een "goed beveiligd telefoonnet".

Wij als redaktie hebben deze truuk natuurlijk nog nooit uitgeprobeerd, en als je het wilt proberen doe je dat NATUURLIJK op eigen verantwoordelijkheid. We no nothing, we are from Barcelona.

Reacties op dit artikel zullen worden doorgestuurd naar de auteurs.

CELLEN ONTAARD

Wie een beetje creatief telecommuniceert heeft nachtmerries van maar 1 ding: zijn kostenteller. Elke tik is een nagel aan de doodskist van de phreak. Als je er maar lang genoeg door geterroriseerd bent ga je je vanzelf afvragen hoe zo'n teller nou eigenlijk werkt.

De techniek werkt als volgt: een telefoonlijn heeft 2 signalen, genoemd 'a' en 'b'. Verder is er in het hele telefoonnet nog een gemeenschappelijke aarde. Deze aarde is voor het voeren van een gesprek niet nodig, maar voor het detecteren van de kostentik (die slechts t.o.v. aarde te meten is) is hij absoluut noodzakelijk. De kostentik is namelijk een korte wisselspanning van 50 Hz op zowel "a" als "b" t.o.v. aarde.

Doorknippen die aarde zou je zeggen. Het probleem is dat de PTT de kosten al in de centrale registreert en het de centrale een worst zal zijn of jouw teller meeloopt, zolang hun teller maar loopt. Er zijn echter ook telefoonlijnen waarbij de detectie van de tellertik bij het toestel WEL uitmaakt: bij telefooncellen!

Blijft de vraag hoe je bij de aarddraad van zo'n cel komt. Laten we eens een cel uit elkaar halen: De "standaard" telefooncel bestaat uit de volgende elementen:

- 1 x saai groen huisje met semi-modern PTT logo en rottig opengaande deur (glas (indien aanwezig) onder de graffiti)
- 1 x TL verlichting (meestal stuk, of hinderlijk knipperend)
- 1 x gebruiksaanwijzing in 4 talen
- 1 x telefoontoestel met muntinworp (toestel wisselt niet!)
- 1 x geldkluis, goed genoeg om Nederlandse goudvoorraad in op te slaan
- 1 x kastje met stoppen en telefoonaansluiting, slecht genoeg beveiligd om met een eenvoudig driehoeksleuteltje geopend te worden. Verder uitermate geschikt om met je voeten op te leunen als je aan het bellen bent (met Tokio).

In sommige cellen zit om de geldkluis en de kast met aansluitingen een groene ombouw met ronde sloten. Helaas hebben we de sleutels van deze sloten nog niet, dus tot die tijd kun je die cellen wel vergeten.

Back to business

Dit verhaal draait dus om de groene voetsteun; de kast met stoppen en een telefoondraad. Deze kast kun je met een driehoeksleuteltje opnamaken. Het is echter een nogal klein driehoekje en er is niet veel ruimte voor de sleutel. Vraag bij een goed gesorteerde sleutelboer naar een sleutel om parkeerpaaltjes open te maken, die zijn in de meeste gevallen goed genoeg. Past ie niet dan wil bijvijlen ook helpen.

Een foto van de kast zonder deksel is bijgevoegd.

Links in deze kast zie je een stoppenrek met zekeringen voor de verlichting en de stroomvoorziening het toestel. Het stoppenrek doet wat overdreven aan, maar de kast hangt direct op de stroom-hoofdkabels, dus een beetje extra voorzorg is nooit weg. Wij hebben er in ieder geval geen last van.

Rechts naast alle electra onzin zit een ronde ijzeren huls. In deze huls verdwijnt een dikke PTT aansluitkabel (blauw). Er uit komt een dunne grijze draad, die naar het toestel loopt: de telefoonlijn!

Als je deze draad met een mesje opensnijdt (in de lengterichting, anders maak je de zaak kapot) zie je 5 geisoleerde adertjes.

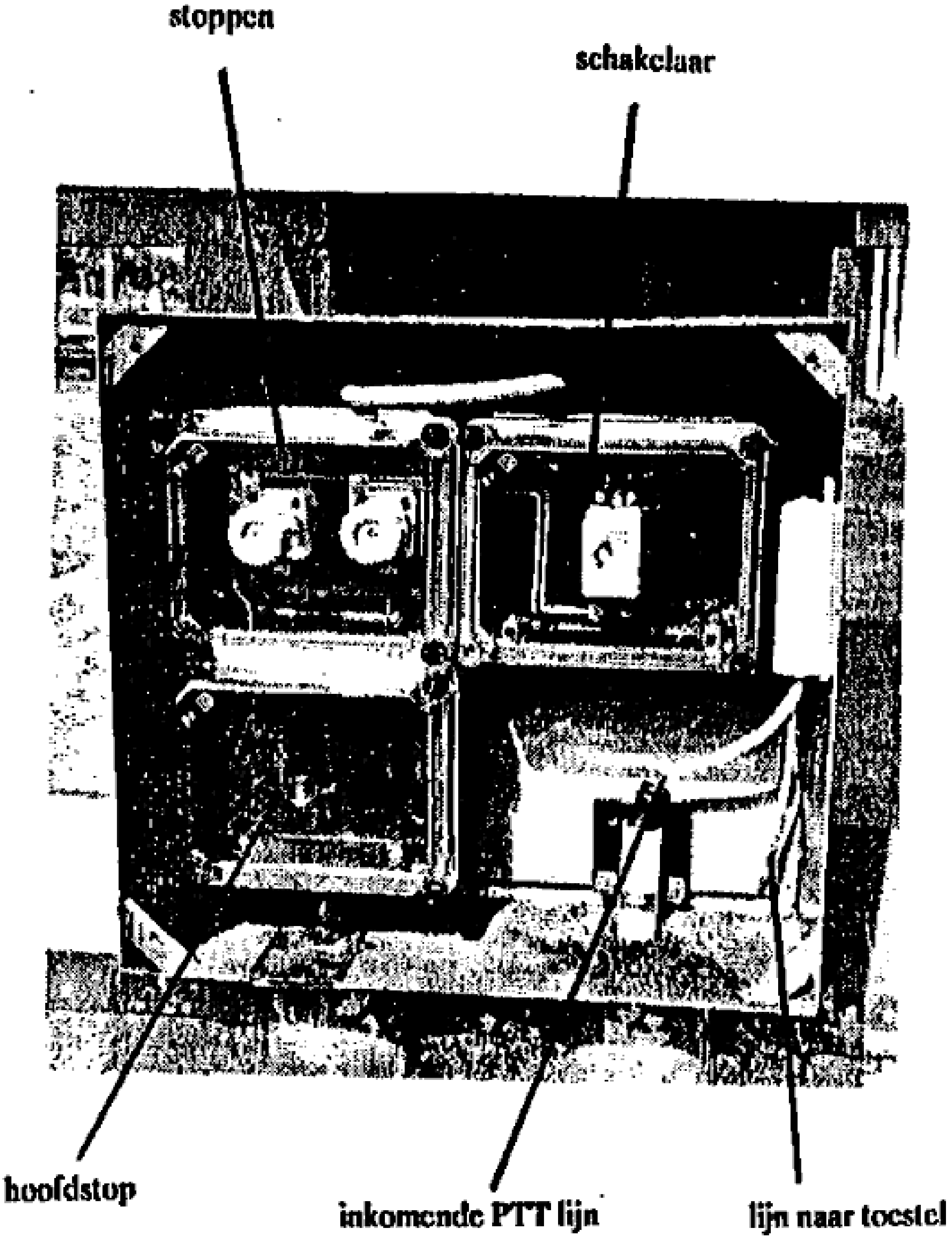
- Rood - "a" draad telefoonlijn
- Blauw - "b" draad telefoonlijn
- Groen - ongebruikt
- Geel - ongebruikt
- Transparant - Aarde (!)

Met een tangetje knip je de doorzichtige draad door, je sluit de kast weer af en klaar is Kees. Je kunt nu wel bellen maar de kostenpulsen komen niet meer door. De cel zal dus ook geen kwartjes meer doorslikken en het ingeworpen kwartje komt na 1.5 uur bellen met de USA gewoon terug (kick!).

Als je het op deze manier doet kan iedereen dus gratis bellen in die cel. Dat is natuurlijk een mooi geschenk aan de bevolking maar het nadeel is dat de pret niet bijster lang duurt. Je kunt natuurlijk ook een magneetkontakje monteren. Je legt een magneet bovenop de kast en het kontakje verbreekt de aarde. Haal de magneet weer weg en de cel detecteert weer elke kostentik. Eventueel is een geniepig klein schakelaartje ook goed, maar de kans bestaat dat anderen dit zien zitten. Als je geld over hebt kun je zelfs de basisunit van een draadloze telefoon inbouwen, dan hoef je de deur niet meer uit!

Have Phun.

De Trunk-Junks


stoppen
schakelaar
hoofdstop
inkomende PTT lijn
lijn naar toestel

Megascan

Hack-Tic is van plan om samen met de lezers verschillende projecten op te starten, zo zijn er plannen om een packet-radio netwerk voor hackers op te starten (packet-radio: modemgebruik via een (in dit geval legale 27 Mc) zender). Geinteresseerden voor dit project kunnen een briefje sturen aan de redaktie zodat wij kunnen zien of er animo voor is.

Scanproject

Zo willen we ook gecoordineerd gaan scannen. Scannen is het op zoek gaan naar modemtelefoonnummers en andere leuke dingen door botweg proberen. Op dit moment zoeken wij mensen die mee willen werken aan de grootste scan die ooit in Nederland gehouden is. Het is dan de bedoeling om al deze gegevens samen tevoegen in een lijst en deze lijst dan te verspreiden onder de mensen die meegewerkt hebben aan deze "Megascan".

Waarom?

Uit ervaring weten we dat er veel mensen zijn die bepaalde nummers scannen, zo zijn er bijvoorbeeld veel mensen bezig met (gratis) 06-nummers. Het is gewoon zinloos om deze nummers meer dan een keer te bellen. Beter is het om je te organiseren, ieder een gedeelte voor je rekening te nemen en later de informatie uit te wisselen.

Software

Veel van onze lezers beschikken over een computer en een modem. Om te kunnen scannen heb je behalve deze twee ook nog een scanprogramma nodig. Voor de IBM-PC, de Amiga en andere bekende merken zijn zulke programma's wel te krijgen, probeer hiervoor ook de grote bulletin boards.

Het is ook mogelijk om met de hand te scannen (voor bepaalde series verdient het zelfs de voorkeur). Als je dus op je werk niets te doen hebt....

Werkwijze

Indien je wilt meewerken aan deze scan moet je een briefje schrijven aan Hack-Tic (zie voor adres het colofon), onder vermelding van :

- Naam
- Adres
- Computer, modem, software
- Eventuele opmerkingen

Nadat wij alle post verwerkt hebben zullen wij vanaf het volgende nummer het gekozen scangebied gaan opdelen onder de scanners. Waarna wij in de daarop volgende nummers steeds verslag zullen uitbrengen over de vorderingen van de Megascan. Niet scannende abonnee's krijgen slechts een deel van de gevonden nummers: het moet de moeite lonen om mee te doen!

Doorschakelen

Je hebt wel eens van die fantasieën over het in de war schoppen van het telefoonnet. Ons gebeurt het vooral als we iets gedaan willen hebben van de PTT en de vijfde telefoniste vraagt ons vriendelijk of we een momentje hebben. Als je dan wilt uitleggen dat dit niet het geval is blijkt ze reeds verdwenen. Op dit soort momenten zou je willen dat je de nummers van alle telefoonaansluitingen kon omdraaien. Nu heeft de PTT in zijn nieuwere centrales zoiets ingebouwd.



De telefooncentrales die nu worden geplaatst bestaan uit lange, saaie kasten waar telefoonlijnen uitkomen. Nergens is meer geratel van relais te horen, de lucht ruikt niet meer naar soldeerhars en smeerolie. De oude rot in het vak is vervangen door een jonge computertechnicus achter een terminal. Het hart van de centrale is een computer. Voor de telefoongek heeft dit alles echter ook voordelen.

Dit artikel gaat over het eerste type computergestuurde centrale, de PRX. Deze PRX was nog niet geheel digitaal; de spraak liep nog over kleine, computergestuurde relais. Het kiezen was echter al volledig digitaal en als je op een PRX bent aangesloten kun je kiezen door middel van DTMF (zie Hack-Tic 2).

De computer van een PRX leest zijn programma van tape, een zogenaamde "load-tape". Op de oude versie van deze tapes zat een geintje: het was mogelijk om een telefoonnummer door te schakelen. Op deze manier kon je alle gesprekken voor een bepaald telefoonnummer terecht laten komen op een andere lijn.

Sinds enige tijd biedt de PTT deze service ook aan abonnee's, maar dat werkt anders. Als je op deze service bent geabonneerd kies je "*21*telefoonnummer#" en dan komen al je telefoongesprekken op het ingetikte telefoonnummer terecht. Als je gebeld wordt gaat eerst de doorgeschakelde telefoon 3 maal over en dan pas wordt het ingetikte nummer gebeld. Als je dit weer uit wilt zetten tik je "#21#".

De grap waar we het hier over hebben werkt echter met 3 cijfer codes, zoals "*999*telefoonnummer#". De doorschakeling komt ook onmiddelijk tot stand: het doorgeschakelde toestel rinkelt helemaal niet meer. De gebruikte codes verschillen van centrale tot centrale. Hoe kom je er achter of zoiets op jouw centrale mogelijk is?

test je centrale...

Neem de telefoon op en druk op het sterretje. Er zijn 3 mogelijke reacties van de centrale:

- Je hoort een telefoon 3 maal overgaan, daarna wordt er opgepakt en hoor je een toon. Dit is de zogenaamde ATEMA testpiep en geen computercarrier. Pech, jouw centrale is saai.

- Je krijgt onmiddelijk de informatietoon (toe-doe-diep). In dit geval is je centrale HEEL saai, hier zijn geen geintjes mogelijk

- Het blijft stil. Je drukt 20 en je krijgt een twwede kiestoon alsof je net een netnummer hebt gedrukt (vooral in Amsterdam populair). We weten hier nog nietr genoeg van, maar het lijkt niet veel mogelijkheden te bieden.

- Het blijft stil en het bovengaande gaat niet op. Dit kan interessant zijn; doe het volgende experiment:

Druk op het cijfer 1. Krijg je nu gelijk de informatietoon dan leg je neer en probeer je het met het cijfer 2. Er zou (als jouw centrale gevoel voor humor heeft) 1 getal moeten zijn wat weer leidt tot een stilte. Stel even dat dit het cijfer 3 is. Dan ga je verder

met *31, *32, *33 enz. enz. Dit doe je net zo lang tot je een combinatie hebt die weer een stilte geeft. Zoek dan volgens dezelfde methode het derde cijfer en je hebt de code gevonden (max. aantal mogelijkheden = 30 !).

Als de gevonden code 321 is dan tik je dus "*321*tel.nummer#" om door te schakelen. Je hoort dan een "gebroken" kiestoon. Dit is de gewone kiestoon met om de seconde een korte stilte. Leg nu neer, pak weer op en bel je eigen nummer. Je krijgt dan geen bezettoon, maar een gesprek met het ingestelde nummer.

Je kunt elk nummer instellen, met als enige beperking dat het een nummer binnen Nederland moet zijn. 06-nummers (ook de dure), mogen echter wel, zodat je tegen lokaal tarief naar allerlei koopnummers kunt bellen.

Alle anderen die dit nummer bellen krijgen echter ook het door jou ingestelde nummer. Vergeet dus niet om na elk gesprek de zaak weer terug te zetten. Dit gaat met "#code#" waar code weer staat voor de door jou gevonden drie cijfers.

Opgelet: er zijn centrales waar de uitschakelcode een andere is dan de inschakelcode. Er zijn (waren?) ook centrales waar je wel kunt doorschakelen, maar niet meer terug. Verder gaan er verhalen van idioot hoge telefoonrekeningen door dit geintje; op onze telefoonrekeningen heeft dit alles echter slechts een verzachtende invloed gehad.

The Key & Peter Poelman

(Het is duidelijk dat de telefoon door steeds meer aktiegroepen wordt onderkend als middel om "iets van je te laten horen". Dezelfde advertentie stond ook in de dagbladen, maar dan met het landelijke nummer van Shell in Den Haag.)

Bel Shell uit Zuid-Afrika



Allan Boesak zegt 'Met Shell-benzine gevulde voertuigen terroriseren onze mensen. Shell moet zich terug trekken uit Zuid-Afrika, hoe eerder hoe beter!'

Bel op dinsdag 9 mei
het Koninklijke Shell Laboratorium Amsterdam en vraag Shell zich terug te trekken uit Zuid-Afrika.

Telefoon:
020-309111
020-303081

organisatie Novib, Pax Christi, Kairos, Komitee Zuidelijk Afrika
informatie O.Z. Achterburgwal 173, 1012 DJ, Amsterdam.

In de tijd dat de ptt steeds de schuld krijgt van fraude met telefooncellen en telefoonrekeningen blijkt dat een gedeelte van de te hoge rekeningen niet de schuld is van de ptt, maar van de abonnee zelf. Deze abonnee is bezitter van een draadloze telefoon en zonder het te weten legt hij/zij de toegang tot de telefoonlijn bloot.

Draadloze telefoon

Door: Tx

De draadloze telefoon is zoals de meesten van jullie zullen weten een telefoon waarmee je ongeveer 200 meter rond het huis kunt bellen. Deze telefoons, meestal afkomstig uit het verre oosten, zijn officieel bedoeld voor de Amerikaanse markt, en wordt via ons land daar naar toe verscheept. Eenmaal in Rotterdam aangekomen wordt een gedeelte appart gehouden voor de verkoop op de Nederlandse markt. Hoewel justitie ongeveer 2 jaar geleden de verkoop van deze telefoons heeft verboden worden ze nog iedere dag in grote getale verkocht via dagbladen en op markten.

Om deze illegale telefoons zo goedkoop mogelijk te houden is er geen lijnbeveiliging ingebouwd zoals bij de duurdere en meestal goedgekeurde types (bij de ptt verkrijgbaar voor belachelijk hoge prijzen). Deze beveiliging is bij de duurdere illegale types een eenvoudig kodeersysteem wat het onmogelijk maakt om, zonder de goede kode in de handset te hebben ingesteld, kontakt te leggen met de basis.

De oplossing van de ptt

De oplossing van de ptt voor hun goedgekeurde toestellen (type: New York) was heel simpel: door een systeem in te bouwen dat om de 14 seconden een pieptoon van de handset naar de basis stuurde en visa versa kon de basis controleren of de handset van de rechtmatige eigenaar werd gebruikt. Echter door het uitzenden van deze pieptoon waande je je eerder in een gokhal dan in een telefoongesprek.

Nog een nadeel

Draadloze telefoons hebben nog een nadeel, ze zijn door iedereen met een beetje uitgebreide scanner eenvoudig af te luisteren. Ook hier had de ptt een oplossing voor, de telefoons werkten op verschillende frequenties in de buurt van de 900 mhz, zodat de ptt telefoon volgens de folder niet af te luisteren was zonder daar voor de nodige ingewikkelde en dure apparatuur in huis te hebben. Leuke verkoopstunt, maar niet waar. Een beetje radio amateur heeft wel de benodigde ontvanger in huis en

voor hem is het dus zeer eenvoudig om deze gesprekken af te luisteren.

Nieuwe telefoon

De ptt was echter ook op de hoogte van deze nadelen en de telefoon werd waarschijnlijk ook niet zo goed verkocht zodat er een 2e type op de markt komt (de Sydney). Volgens mijn bron bevat deze telefoon een microchip die om de minuut een andere frequentie kiest, waardoor je niet meer kan worden afgeluisterd en er niet meer op jouw kosten gebeld kan worden (kosten van deze telefoon zijn waarschijnlijk weer volgens het veel te hoge ptt 'grijp de winst' tarief).

De goedkope telefoon

De goedkope illegale draadloze telefoon bevat zoals eerder opgemerkt geen lijnbeveiliging zodat er via zo'n telefoon gratis gebeld kan worden. Het principe is heel eenvoudig, wanneer wij de basis van onze telefoon uitzetten en de handset aan, dan ontvangen wij geen signaal meer van onze basis maar van een basis uit de omgeving (wanneer er een in de buurt is en deze op dezelfde frequentie werkt als onze telefoon). Horen we een kiestoon dan kunnen we dus gratis bellen.

Opmerking 1: De basisset van de 'buurman' moet dus wel standby staan, d.w.z. dat de telefoon niet op de lader ligt, want in dat geval is de basis uitgeschakeld (de telefoon wordt toch niet gebruikt, want die ligt te laden). Slim van de uitvinder en jammer voor ons, want dit betekent dat je niet altijd over je gratis telefoon kunt beschikken.

Opmerking 2: De draadloze telefoon kan alleen in de late uren worden gebruikt omdat anders de eigenaar de lampjes op de basis ziet knipperen en eventueel het relais hoort klapperen. Denk er ook aan dat bij een simpel doorgetrokken telefoonleiding alle telefoons in het huis gaan meerinkelen.

Opmerking 3: Mensen die de draadloze telefoon naast hun bed hebben liggen als 2e telefoon zijn het makkelijkste slachtoffer. - Naast het bed gaat geen telefoon meerinkelen wanneer jij kiest. - De telefoon ligt niet op de lader, want is voor de nacht opgeladen.

Afluisteren

Naast het gratis bellen is het ook goed mogelijk om deze telefoons af te luisteren, de frequenties bevinden zich meestal tussen 46 en 50 mc en rond de 70 mc hoewel er op de kortegolf rond 1.7 mc ook telefoons te horen zijn. Een lijst van veel gebruikte frequenties :

	basis	handset
1	46.610	49.670
2	46.630	49.845
3	46.670	49.860
4	46.710	49.770
5	46.730	49.875
6	46.770	49.830
7	46.830	49.890
8	46.870	49.930
9	46.930	49.990
10	46.970	49.970

Hier een lijstje met de frequenties van 'kortegolf' telefoons.

1	1.705	49.830
2	1.735	49.845
3	1.765	49.860
4	1.795	49.875
5	1.825	49.890

De niet af te luisteren telefoon van de ptt (type New York) is te horen in het volgende gebied :

basis	handset
+/- 959-960	+- 914-915

Verboden

Tot slot wil ik iedereen er op wijzen dat het hebben van een zender (draadloze telefoon) en het gebruik bij de wet verboden zijn.

Artikel 3 lid 1 van de telegraaf en telefoonwet:

"Een machtiging van de Minister is vereist voor de aanleg, het aanwezig hebben en het gebruik van radio-electrische zendinrichtingen"

Een gids voor VMS

(de beginstappen in het VAX/VMS operating systeem)

Door: John D.

(Ik schrijf deze serie omdat ik vaak meemaak dat hackers in een systeem zitten en er de ballen verstand van hebben, waardoor ze of het systeem vernielen en soms maanden werk kapotmaken of een ongoing hack voor anderen om zeep helpen. Ik hoop dan ook dat deze uitleg kan bijdragen tot wat meer inzicht in het systeem en in wat je wel en niet kunt doen.)

De Vax computer wordt door DEC (Digital Equipment Corp.) gemaakt en er kunnen verschillende besturingssystemen op draaien. In dit artikel zal ik ingaan op het VMS besturingssysteem (Virtual Memory operating System).

Toegang

Wanneer je voor het eerst kontakt maakt met een VAX zal die (eventueel na RETURN, CTRL-Y of CTRL-C) ongeveer als volgt reageren:

VAX II
VESTA Chemicals Proto type and ATLAS development Node:
VESVAX

Username:
Password:

De meest gebruikte manier om toegang te krijgen is door gebruik te maken van een 'standaard'-login/password. In het bovenstaande voorbeeld zou je VESVAX als gebruikersnaam kunnen proberen met password VESTA, of een andere combinatie van woorden die in het 'welkomstwoord' staan. ATLAS/ATLAS, VESVAX/VAX, enz.

Wanneer DEC een nieuw systeem bij de klant aflevert, zijn er al een stel standaard accounts ingebakken, met een gebruikersnaam en een password:

Een paar hiervan zijn:

- DEFAULT - Dit wordt gebruikt als voorbeeld om nieuwe users 'aan te maken in de UAF (Users Access File) Een nieuwe gebruiker (user) krijgt de waarden van de DEFAULTgebruiker, tenzij de systeem-beheerder de gebruiker andere waarden wil geven. Het DEFAULT-account kan NIET van de UAF worden verwijderd (en bestaat dus altijd).
- SYSTEM - Hiermee kan de systeemmanager met volledige privileges inloggen. Het SYSTEM-account kan NIET van de UAF verwijderd worden.
- FIELD - Hiermee kan het DIGITAL-field-service-personeel een nieuw systeem controleren. De FIELD-record kan wel verwijderd worden als het systeem eenmaal is geinstalleerd.
- SYSTEST - Hiermee kan het UETP worden (User Environment Test Package)gerund. Het SYSTEST-account kan wel van de UAF verwijderd worden als het systeem eenmaal is geinstalleerd.

Gewoonlijk zal de SYSTEM MANAGER de accounts die in de UAF staan als het systeem zijn huis binnenkomt, veranderen of verwijderen maar dat is niet altijd waar. Soms vergeet hij het of weet hij het niet of denkt hij zowieso niet aan beveiligen.

De standaard passwords die wel eens willen werken zijn:

Username:	Password:
SYSTEM	MANAGER of OPERATOR
FIELD	SERVICE of TEST
DEFAULT	USER of DEFAULT
SYSTEST	UETP of SYSTEST

Ook typische VMS-accounts zijn:

VAX	VAX
VMS	VMS
DCL	DCL
DEMO	DEMO
TEST	TEST
HELP	HELP
NEWS	NEWS
GUEST	GUEST
GAMES	GAMES
DECNET	DECNET
DBMS	DBMS
MRGATE	MRGATE

en verder namen van grote programma's die wel eens op VMS draaien.

Bovenstaande accounts kunnen in een willekeurige combinatie voorkomen. Als je hierna nog steeds niet binnen bent, dan wordt het tijd te verhuizen naar het volgende systeem, tenzij je een andere mogelijkheid ziet om aan een geldige username en password te komen: b.v. door de vuilniszakken van het bedrijf na te kijken, of op te bellen met een of ander verhaal etc. Kortom: research is dan geboden.

Dat je binnen bent herken je aan het feit dat er een nieuw welkomst bericht over je scherm rolt of door de prompt: $ (dollarteken). (Een enkele keer krijg je ook wel eens een andere prompt, die van te voren gedefinieerd is: zoiets als in een autoexec-file op de PC.)

Als je inlogt, wordt je automatisch in een directory gezet, die door de systeembeheerder is vastgesteld. Die defaultdirectory hoort bij jouw account (= username)).

Als je inlogt als systeembeheerder heb je volledige toegang. Als je binnenkomt onder de FIELD of de SYSTEST-account kun je al dan niet volledige toegang hebben, maar je zult in dat geval altijd het privilege hebben om jezelf volledige toegang te geven. Om te zien welke privileges je hebt: $ SHOW PROCESS/PRIVS Om jezelf al deze privileges te geven: $ SET PROCESS/PRIVS = ALL. Als je eenmaal volledige privs hebt kun je elke directory en elke file die je wilt benaderen en bovendien het AUTHORIZE-programma runnen, dat een volgende keer uitgelegd zal worden.

Het VMS-systeem staat vol helpfiles die je op je scherm kunt krijgen door HELP in te typen. Je kunt een wildcard (*) gebruiken om info over elk commando te krijgen: `$ HELP *`.

Als je net binnen bent, is het wel eens makkelijk om een overzicht te hebben van de mensen die op dat moment ook ingelogd zijn: Je kunt dit krijgen d.m.v.: `$ SHOW USERS`. Je zou dan iets dergelijks moeten krijgen:

```
VAX/VMS Interactive Users
      - Total = 4
01-DECember 1988 :
              11:37:21.73

OPA0:DEMO       004C004C
TTD2:LAUREN     0059004A
TXB1:FIELD      08D004E
TXB3:PIETVK     01190057
```

Het is aan te raden, als je overdag ingelogd bent en er meerdere gebruikers ingelogd zijn (in het bijzonder de systeembeheerder of de operator) uit te loggen en later terug te bellen. Soms kan de dageraad echter als dekmantel dienen als er veel gebruikers bezig zijn: vooral als je onder een niet-opvallend account binnengekomen bent. Tot nu toe is mijn ervaring echter dat de beste manier om niet op te vallen is te bellen als er niemand op het systeem zit. ('s nachts en in het week-end dus)

Om met andere gebruikers of hobbygenoten op het systeem te praten doe je:

$ PHONE. (Er is uiteraard ook HELP PHONE aanwezig)

Als het systeem aan Decnet vastgeknoopt zit kun je een overzicht van de andere computers (= NODES) krijgen d.m.v.:

$ SHOW NETWORK .

Om namen van ingelogde gebruikers op die andere systemen te zien:

$ PHONE en als je 'in phone' bent: DIR NODENAAM

Als je post hebt zal het systeem dit netjes aan je melden wanneer je inlogt. Lezen doe je met $ MAIL . Dit is het persoonlijke postprogramma, waarbinnen een uitgebreide help-file zit. Postbestanden in je directory kun je herkennen aan: MAIL.MAI, of andere vormen waar 'MAI' zowel in de filenaam als in het filetype staat. Om te zien of er iets van post in je directory staat: $ DIR MAI*.*;*. VMS staat het gebruik van wildcards toe: '*' voor meerdere karakters, '%' voor exact een karakter. Het sterretje achter de puntkomma bij MAI*.*;* staat voor het versienummer van die file.

Het systeem barst van de commando's en een heleboel zijn voor hackers niet interessant, dus zal ik niet al te veel in detail gaan. Een ding over VMS: er is genoeg hulp aanwezig in de vorm van het HELP-commando. Daar staat voldoende in om het systeem redelijk onder de knie te krijgen.

Directories

Files staan in directories en die staan weer op schijven; het kunnen vaste schijven zijn, maar ook verwisselbare. Wat ook voor kan komen zijn magneetbandapparaten. Om een file te benaderen in een bepaalde directory en op een bepaalde schijf, moet je eerst de schijfnaam noemen, dan de directory en dan de file die je wilt bekijken: bijv:

$ TYPE schijfnaam:[dirnaam]filenaam.filetype;versienummer

voorbeeld:

TYPE DUA0:[piet]tel.nrs;2 (Piet zit op schijf DUA0 en van hem wil je de tweede versie van zijn file 'tel.nrs' bekijken.

Op dezelfde manier kun je ook directories op andere schijven benaderen: $ DIR schijfnaam:[dirnaam] of default zetten ('er naar toe gaan'): SET DEFAULT schijfnaam:[dirnaam].

Schijfnaam en directorynaam kun je ook weglaten: dan gelden je default schijf en je default directory. Dus om te zien wat er in je eigen directory staat tik je: $ DIR[*.*].

Niet alle vaxen gebruiken dezelfde namen voor de schijven: SHOW DEVICES geeft een aardige indicatie. Daarnaast heb je ook nog het commando SHOW LOGICAL waarmee je ook een idee kunt krijgen waar bepaalde files te vinden zijn. Als je het gewone DIR-commando geeft, krijg je de systeem- directories niet te zien. Deze zijn al geïnstalleerd wanneer de VAX wordt afgeleverd:

- [SYSLIB] - verschillende macro en object-bibliotheken,
- [SYSMSG] - systeemberichten files
- [SYSMGR] - files om het om het operating systeem te beheren
- [STSHLP] - tekstfiles en de help bibliotheken voor het HELP-commando
- [SYSTEST]- files gebruikt om het operating systeem te testen [SYSMAINT]-system diagnostic programma's
- [SYSUPD]- files die gebruikt worden om updates in te voeren
- [SYSEXE]- programma's van de meeste systeemfuncties.

Deze directories bevinden zich in `SYS$SYSROOT:[000000]` en zijn dus subdirectories van de hoofddirectory `[000000]`. Binnen deze directories kunnen files van de volgende typen voorkomen:

- .txt - ASCII-tekst file
- .hlp - systeem help-file
- .dat - data-file
- .msg - bericht-file
- .doc - documentatie
- .log - log file
- .err - foutbericht-file
- .seq - sequentiele file
- .mai - post-file
- .sys - systeemfile (runnen met `$ FILE_NAAM`)
- .exe - executable file (runnen met `RUN FILENAAM` of `RUN SYS$SYSTEM:FILENAAM`
- .com - command-file (runnen met `COMMAND FILENAAM` of: `@ FILENAAM`
- .dir - directory

Er zijn nog wel meer typen te vinden, maar bovenstaande zijn de meest voorkomende. Je kunt van directory veranderen door:

`$ CHANGE [DIR.NAM]` of: `$ SET DEFAULT [DIR.NAM]`

Soms heb je niet genoeg privileges om naar een andere directory over te stappen. Je kunt soms toch files hierin listen door: `TYPE [PIETERS]mail.mai;1`.

Hiermee krijg je de postfile van user Pieters op je scherm (als die tenminste niet beveiligd is).

Om in een subdirectory te komen: `$SET DEFAULT [DIRNAAM.SUBDIRNAAM]` Om een nivo hoger te komen `SET DEFAULT [-]` een niveau lager `SET DEFAULT [.]`

Gevonden in SARA-bulletin, van de Stichting Academisch Rekencentrum Amsterdam:

TRICKLE@TREARN

Trickle is een fileserver voor MS-DOS-software. Trickle is op meer plaatsen geïnstalleerd, maar voor ons is TREARN (Izmir, Turkije) in netwerkbegrippen het dichtstbij. Eenzelfde server bevindt zich in Antwerpen maar dat is voor EARN tweemaal zo ver van SARA als Izmir. Stuur voor meer informatie een mail of interactieve message met de opdracht

/HELP

Internationale netwerken

In den beginne was er niks...Toen vond men de computer uit. Na een tijdje wilde men computernetwerken hebben. Ongecoordineerd begon men die te bouwen. En toen....was er CHAOS! De wildgroei maakt dat niemand meer precies weet hoe en wat, maar dat maakt het eigenlijk wel zo gezellig. In dit artikel wil ik proberen een klein beetje licht in de duisternis te werpen. Puntgewijs zal ik een aantal netwerken aflopen. Networks, here we come...

Door: Taco

Surfnet

Surfnet is een netwerk dat Nederlandse universiteiten en instellingen met elkaar verbindt. In 1986 is dit begonnen en anno nu is het al een fiks bedrijf. Via surfnet is het mogelijk post en files te versturen en ontvangen, interactief te werken en RJE te doen. RJE staat voor Remote-Job-Entry, oftewel het laten draaien van een batchjob op een andere computer (toch nog eens pi uit rekenen op de CRAY supercomputer van het ENR). Ook is het mogelijk vanaf Surfnet berichten te versturen naar andere netwerken, zoals het EARN-netwerk, dat weer contact heeft met ARPA, JANET en UUCP. Surfnet loopt via Datanet 1 (zie ook Tic-3). In plaats van een nua wordt een zgn mnemonic ingetypt, een verkorte, makkelijk herkenbare naam. Je belandt dan bij de computer en als je dan nog een login hebt kan je naar binnen. Als je eenmaal binnen bent kan je vandaar uit dingen versturen en RJEen.

De adressering binnen DECNET is 'username::nodename'. DECNET is het netwerksysteem van Digital waarvan Surfnet gebruik maakt, voor de VMS. Voor VM/CMS is het 'username at nodename'.

Arpanet

Arpanet is het 'Advanced Research Projects Agency Network', een Amerikaans netwerk met veel overheid en defensie-gein. Arpanet maakt deel uit van een nog groter netwerk, ARPA Internet geheten. Hetzelfde is het geval met MILNET en CSNET.

De adressering is 'userid@domain3.domain2.domain1.domain', waarbij domain3 het laagste in de boomstructuur is. Bv. 'pietje@afdelingvax.universiteit.district.EDU'.
Er zijn verschillende topdomeinen: Op de volgende pagina vind je een overzicht.

Janet

Janet is de Britse tegenhanger van Surfnet, dus een netwerk tussen universiteiten en instellingen. Dit zaakje draait al vanaf 1984. Janet maakt deel uit van EARN, maar heeft een ander protocol, zodat je alleen via een 'gateway' van de een naar de ander kan gaan. Een 'gateway' is, zoals de naam al zegt, een poort naar buiten, in dit geval dus naar een ander netwerk. Deze gateway staat in het Rutherford Laboratorium (EARN-knooppunt UKACRL).

De adressering heeft twee mogelijkheden, te weten eentje van binnenaf en eentje van buitenaf. Als je van binnenaf wilt adresseren ziet het er als volgt uit

'userid@UK.AC.subdomain1.subdomain2', waarbij subdomain2 dus het laagste is. Als je van buitenaf komt is de adressering 'userid@subdomain2.subdomain1.AC.UK', waarbij subdomain2 weer het laagste is. 'UK' staat voor United Kingdom en 'AC' staat voor Academical.

ARPA topdomeinen

- COM : commerciele organisaties
- EDU : onderwijs instellingen
- GOV : civiele regerings organisaties
- MIL : departement van defensie - militaire klanten
- NET : administratieve organisaties voor netwerken
- ORG : andere organisaties
- US : departement van defensie - USA klanten
- XX : tweeletterige landencode voor landen buiten de USA, bv NL

UUCP

UUCP staat voor Unix-to-Unix-CoPy. UUCP is in drie grote delen opgesplitst, te weten voor Europa EUnet, voor Amerika Usenet en voor Japan Junet. Hier zullen we het alleen even hebben over EUnet. EUnet draait al vanaf 1982 en heeft nu al zo'n 1300 knooppunten. EUnet heeft een decentrale opbouw, elk land heeft z'n eigen gebruikersgroep. In Nederland is dat NLUUG. EUnet heeft gateways naar JANET, EARN/BITNET, ASCnet en natuurlijk naar Usenet en Junet. Het knooppunt dat de verbinding onderhoudt tussen EUnet en Usenet en Junet heet mcvax en staat in Amsterdam. Via EUnet is het mogelijk berichten en files te versturen en mee te doen aan electronic conferencing. Het protocol is het UUCP programma van UNIX.

UUCP kent 3 adresseringsvormen:

- user@destination : de meest voorkomende en gewenste vorm.
- destination!user : in mindere mate voorkomend.
- backbone!destination!user : eerst wordt naar het knooppunt verwezen.

Welke vorm je moet gebruiken hangt af van de mailer die het systeem heeft. De laatste vorm wordt gebruikt bij de systemen die alleen standaardsoftware hebben.

EARN

Het EARN (European Academic and Research Network) is het netwerk dat Europese universiteiten en instellingen met elkaar verbindt. Het protocol binnen EARN is RSCS van IBM. EARN heeft een centrale opbouw, ieder land heeft een eigen netwerk dat via knooppunten aan elkaar verbonden is. Die computer (een IBM/VM) verzorgt de communicatie naar de andere knoopunten en geeft allerlei informatie over het nationale netwerk. Een paar namen van die netwerken zijn CEARN (Zwitserland), DEARN (BRD), EEARN (Spanje), HEARN (Nederland) en IEARN
(Ierland).

De adressering is voor VM/CMS 'user at node'. Voor VMS is het, vanuit de mail-utility: jnet%"user@node

SPAN

SPAN staat voor Space Physics Analyzing Network. Hierop zitten allerlei computers van instellingen die met ruimtevaart bezig zijn (ESA, NASA, CERN etc). De Nederlandse toegang staat bij ESTEC in Noordwijk.

In volgende Tic's komt elk netwerk nog een keer uitvoerig aan bod, met alle commando's en mogelijkheden en hier en daar de noodzakelijke verduidelijking.

Portofoon gezondheidsrisico

In Amerika is op het moment een discussie gaande over de gevaren van draagbare autotelefoons, portofoons en andere zend/ontvangapparatuur. Een onderzoek heeft bijvoorbeeld aangetoond dat onder politiemensen meer dan gemiddeld staar voorkomt, en dan altijd aan het oog dat het dichtst bij de kleine portofoonantenne zit.

De politie daar heeft besloten de portofoons nu aan de buikriem te hangen en de agent uit te rusten met een losse microfoon en oorknop. Gevolg: nu krijgen ze balkanker i.p.v. staar.

Zowel door de gebruikte frequenties als door het lage zendvermogen zouden draadloze telefoons niet gevaarlijk zijn.



Aktievoeren per computer

Is je computer een breekijzer?

We ontvingen een brief van een verpleger die zich afvraagt of wij hem kunnen helpen bij het in de war helpen van de gegevensverwerking bij ziekenfondsen etc. Dit alles om de eisen voor een beter salaris en minder werkdruk kracht bij te zetten. Wij van de redaktie zouden er niets tegen hebben de verpleging een handje te helpen, maar we hebben het veel te druk en we weten veel te weinig van ziekenfondsautomatisering.

Het zou ons echter verbazen als er niet 1 abonnee was die net op de juiste plaats zit. We zouden het op prijs stellen als die lezer zich met ons in verbinding stelt. Telefonisch kan ook: 020-6001480.

Of er gereageerd wordt of niet, de verpleging kan gerust zijn: deze brief zal in bepaalde kringen toch wel voor wat transpiratie zorgen.

Beste Redaktie,

Zoals jullie waarschijnlijk wel weten voeren verpleegkundigen en verzorgenden al enige tijd aktie voor een beter slaris en betere arbeidsvoorwaarden.
Het zal jullie ondertussen ook bekend zijn dat het moeilijk is om harde akties te voeren omdat je altijd aan het belang van de patient of bewoner moet denken. Vandaar ook dat wij proberen op allerlei andere vlakken aktie te voeren waarbij we niet de patient maar wel het systeem raken. Zo is al herhaalde malen genoemd dat we eigenlijk iets moesten doen aan de gegevensverwerking bij ziekenfondsen, NZR, WVC etc. Dit zou via inbreken kunnen gebeuren, doch ook d.m.v. het veroorzaken van onrust bij dse genoemde instanties. (het invoeren van het 5% virus)
We hebben geen idee of een en ander ook werkelijk te realiseren is en hoe dit aan te pakken.
Vandaar aan jullie de vraag of jullie enig idee hebben wat we zouden kunnen doen. Dit nog los van de vraag of het zover moet komen.

Antwoorden via de Hack-Tic postbus, wij sturen de zaak dan wel door.